

DDP – A tool for life-cycle risk management

S. Cornford, M. Feather, K. Hicks

Jet Propulsion Laboratory,
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109, USA

At JPL, we have developed, and implemented, a process for achieving life-cycle risk management. This process has been embodied in a software tool and is called Defect Detection and Prevention (DDP). The DDP process can be succinctly stated as: determine where we want to be, what could get in the way and how we will get there. The 'determine where we want to be' is captured as trees of weighted requirements and the 'what could get in the way' is captured as trees of potential failure modes. Failure mode here is used in its most general sense – inability to achieve the requirements. After scoring the impacts of these failure modes on the requirements, one arrives at a prioritized set of failure modes and the risk associated with them. In order to navigate the resultant risk landscape, the user selects from a set of PACTs (Preventative measures, Analyses, process Controls and Tests) each of which has an effectiveness versus the various failure modes. In addition, each PACT also has some resource costs associated with it (e.g. dollars, schedule, mass). It is the goal of the DDP process to optimally select the subset of the PACTs which minimizes the residual risk subject to the project resource constraints.

The DDP process is intended to facilitate risk management over the entire project life cycle beginning with architectural and advanced technology decisions all the way through operation. As the project design, technology content and implementation approach matures, the requirements and failure mode trees are elaborated upon to accommodate the additional information. Thus, the DDP process is a systematic, continuous, top-down approach to managing risk. Implementation of the DDP process requires a critical mass of expertise (usually the project team and a few specialists) and captures both their engineering judgement as well as available quantitative data. This additional data may result from models, layouts, prototype testing, other focused risk evaluations and institutional experiences. The DDP process also identifies areas where additional information would be advantageous, thus allowing a project to target critical areas of risk or risk uncertainty. This also allows the project to identify those areas which would benefit the most from application of other quantitative tools and methods (e.g Monte Carlo simulations, FMECAs, Fault Trees).

The software tool supports the DDP process by providing guidance for implementing the process steps, graphical visualizations of the various trees, their inter-relationships and the current risk landscape. The tool is capable of supporting on-the-fly knowledge elicitation as well as integrating off-line deliberations. There are a variety of available outputs including graphs, trees and reports as well as clear identification of the driving requirements, 'tall-pole' residual risks and the PACTs which have been selected and agreed upon. The DDP process has been applied at various levels of assembly including the system and subsystem levels, as well as down to the component level. Recently significant benefits have been realized from application to advanced technologies, where the focus has been on increasing the infusion rates of these technologies by identification and mitigation of risks prior to delivery to a project.